## *Amendments to the Claims*

The listing of claims will replace all prior versions, and listings of claims in the application.

1.      *(Currently Amended)* A method comprising:

receiving, at a model of a second computer, a status update communication from the second computer, the status update communication including pre-existing information on the second computer;

updating and maintaining the model based on the status update communication, to reflect any changes to the second computer;

receiving computer data from a first computer at [[a]] the model of [[a]] the second computer, the model being having been maintained and updated to reflect any changes to the second one of the first and second computers prior to receiving the computer data;

screening the computer data for at least one virus using the model to produce a screening result; and

communicating the screening result from the model to the second computer.

2.      *(Previously Presented)* The method of Claim 1, further comprising using an IP network for the transmission of the computer data and the screening result.

3.      *(Original)* The method of Claim 1 further comprising:

if the at least one virus is detected, performing at least one of the following:

(i)      inhibiting communication of at least a portion of the computer data to the second computer;

(ii)     removing the at least one virus from the computer data prior to transferring the computer data to the second computer;

(iii)    communicating a message indicating that the at least one virus was detected to the second computer;

(iv)    communicating a message indicating that the at least one virus was detected to the first computer; and

(v)     writing data to a database indicating that the at least one virus was detected.

4.      *(Cancelled)*.

5.      *(Currently Amended)* A virus screening system operative to be connected to a network and operative to screen computer data for at least one virus when the computer data is transmitted between a first computer and a second computer, the virus screening device comprising:

a third computer on the network that comprises a model of a second one of the first and the second computers, the model configured to be maintained and updated <u>prior to receiving the computer data, based on pre-existing information on the second computer,</u> to reflect any changes to the second one of the first and second computers and to screen the computer data from a first one of the first and second computers,

wherein a result of the screening is communicated from the model to the second one of the first and second computers.

6.      *(Original)* The system of Claim 5, wherein the network comprises an IP network.

7.      *(Cancelled)*.

8.      *(Previously Presented)* The system of Claim 5, wherein the network comprises a local area network, wherein the model resides outside the local area network.

9.      *(Original)* The system of Claim 5, wherein the computer data comprises an electronic mail message.

10.     *(Original)* The system of Claim 5, wherein the computer data comprises data requested by the second computer from the first computer.

11-13. *(Cancelled).*

14.     *(Previously Presented)* The method of Claim 1, wherein the model resides within a wide area network, and wherein the method further comprises:

        receiving across a local area network a request for requested data from the first computer;

        sending the request across the wide area network to the second computer; and

        requesting that the requested data be returned via the model.

15.     *(Previously Presented)* The method of Claim 1, further comprising:

        receiving a request for the computer data from the first computer at a modem external to the first computer; and

        initiating communication of the computer data from the modem across an IP network to the second computer.

16-18. *(Cancelled).*

19.     *(Previously Presented)* The method of Claim 1, wherein the model resides within a wide area network, and wherein the method further comprises:

- 5 -
FRANCZEK *et al.*
Reply to Office Action of December 17, 2008
Appl. No. 10/810,443

configuring the model to inhibit communication of executables to the first

computer; and

configuring an electronic mail system associated with the first computer

to route messages addressed to the first computer through the model.

20.     *(Previously Presented)* The method of Claim 1, wherein the first computer is

communicatively coupled to a local area network and the model resides outside a

firewall associated with the local area network, and wherein the method further

comprises:

configuring the model to inhibit communication of executables to the first

computer; and

configuring an electronic mail system associated with the first computer

to route messages addressed to the first computer through the model.

21.     *(Previously Presented)* The method of claim 1, wherein the screening result

comprises a version of the computer data.

22.     *(Previously Presented)* The method of claim 21, further comprising using a

reduced data version, simplified version, or modified version of the received computer

data as the version of the computer data.

23.     *(Previously Presented)* The method of claim 21, further comprising generating a

new installation program as the version of the received computer data.

24.     *(Currently Amended)* The method of claim 21, further comprising generating a

handshake data packet as the version of the received computer program data.

25.     *(Previously Presented)* The method of claim 1, wherein the screening comprises screening a portion of the computer data less than all of the computer data for the at least one virus.

26.     *(Previously Presented)* The method of claim 1, further comprising disabling the screening when the computer data is voice data.

27.     *(Previously Presented)* The method of claim 1, further comprising switching between allowing and disallowing the screening based on enabling and disabling signals within the computer data.

28.     *(Previously Presented)* The method of claim 1, wherein the maintaining and updating of the model comprises determining parameters of the second computer, wherein the parameters comprise a version of an operating system, a hardware type, registry information, configuration information, or information from initialization files.

29.     *(Currently Amended)* The method of claim 1, wherein the maintaining and updating of the model comprises <u>one or more of:</u> requesting information from the second computer, obtaining information from the model if the information was created or altered by ~~the installation program~~ <u>using the model to produce a screening result</u>, and requesting information from a pre-existing image of the second computer<u>.</u>

30.     *(Previously Presented)* The method of claim, 29, wherein the pre-existing image of the second computer mimics a state of the second computer by maintaining a copy of settings and data stored to the second computer.

31.     *(Previously Presented)* The method of claim 1, wherein the receiving, screening, and communicating of the computer data are performed unidirectionally or bidirectionally between the first and second computers.

- 7 -
Reply to Office Action of December 17, 2008

FRANCZEK *et al.*
Appl. No. 10/810,443

32.     *(Previously Presented)* The method of claim 1, wherein at least one of the first computer, the network, or the second computer is subscribed to a service providing the screening.

33.     *(Previously Presented)* The method of claim 1, wherein the model determines from the screening result what is transmitted to the second computer.

34.     *(Previously Presented)* The method of claim 1, wherein the second computer determines from the screening result what is transmitted to the second computer.

35.     *(Currently Amended)* A computer-readable medium containing instructions for controlling at least one processor by a method comprising:

        receiving computer data from a first computer at a model of a second computer;

        maintaining and updating the model <u>prior to receiving the computer data, based on pre-existing information on the second computer,</u> to reflect any changes to the second computer;

        screening the computer data for at least one virus using the model and producing a screening result; and

        communicating the screening result from the model to the second computer.

36.     *(Currently Amended)* A system for transmitting computer data between a first computer and a second computer via a network, comprising:

        means for receiving the computer data from a first computer, the means for receiving being configured as a model of a second computer and being configured to ~~maintain and update~~ <u>be maintained and updated prior to receiving</u>

the computer data, based on pre-existing information on the second computer, for

any changes to the second computer;

      means for screening the computer data for at least one virus;

      means for producing a screening result therefrom; and

      means for communicating the screening result to the second computer.

37.    *(Currently Amended)* A system comprising:

      a processor; and

      a memory storing instructions that cause the processor to:

         receive computer data from a first computer at a model of a

second computer;

         maintain and update the model prior to receiving the computer

data, based on pre-existing information on the second computer, to reflect any

changes to the second computer;

         screen the computer data for at least one virus using the model and

producing a screening result; and

         communicate the screening result from the model to the second

computer.

38.    *(Currently Amended)* A method, comprising:

      causing a an intermediary node to receive computer data from a first

computer, the intermediary node being a model of a second computer;

      causing the intermediary node to be maintained and updated prior to

receiving the computer data, based on pre-existing information on the second

computer, to reflect any changes to the second computer;

causing the intermediary node to screen the computer data for at least one

virus using the model and producing a screening result; and

causing the intermediary node to communicate the screening result from

to the second computer.

39.     *(Currently Amended)* A method comprising:

receiving, at a model of a destination computer, a status update

communication from the destination computer, the status update communication

including pre-existing information on the destination computer;

maintaining [[a]] the model of [[a]] the destination computer prior to

receiving data destined for the destination computer, based on the status update

communication;

analyzing data destined for the destination computer to determine whether

the data includes a virus; and

providing a screening result to the destination computer.